SUNBURY COLLEGE

COLLEGE NETWORK STUDENT CODE OF CONDUCT AND BRING YOUR OWN DEVICE (BYOD) POLICY

(NOTE: The signed agreement form on the last page of this booklet is to be returned with the school enrolment forms)

May 2023

SECTION A

CODE OF CONDUCT

The College offers students the opportunity to enhance their learning outcomes through access to the college computer network, the Internet and other online services as part of the college curriculum. The following guidelines apply to all students.

- Students must have written parental/guardian permission to access the college network.
- Students must sign this agreement in relation to network responsibilities, online access and bringing your own device prior to using the college network.
- Network storage areas (i.e. your personal folder) are for the storage of your files. Only you, your teachers and the network administrators have access to these files. Students are not permitted to block access to their files to teachers and systems administrators.
- Student personal storage areas are for the storage of school-related work only.
- Each student must ensure that the total storage space in their home directories does not exceed the limit authorised by the college.
- Students are to adopt responsible file management practices.
- Users should not expect that files stored on the college's computer servers will always be private.
- Student use of Office 365 and Google Apps for Education is limited to school related activities.

Students are permitted to:

- Use and enjoy the college network as widely as possible to enhance learning. Note that the college's computer resources are for educational purposes only.
- Educational purposes means that students are only permitted to use the college's computers for:
    - Completing class work, assignments, work requirements, projects, VCE school-assessed tasks
    - Researching the online resources for material to complete school work
    - Undertaking any other educational tasks as directed by a teacher.

Specifically, the following actions are not permitted. (Note that this list is not exhaustive. The overriding rule is that students are not permitted to use the computer or internet resources for any purpose, other than those outlined above for educational purposes.)

- Giving your password to another student, using other user's passwords or trespassing in other's folders, work or files.
- Using computer rooms at any time without teacher permission and supervision.
- Eating or drinking in computer rooms or having food or drink in computer rooms.
- Loading games or any other programs/files onto the college network -this applies to all areas of the college network including students' home directories.
- Using email and chat programs other than those authorised by the college.
- Emailing unsuitable sites or material accessed outside of the college to personal email accounts at the college.
- Unauthorised downloading of material from the Internet. This means that students may only download material required for educational purposes as instructed by staff.
- Printing of non-school related material.
- Damaging computers/networks (for example, by the creation, introduction or spreading of computer viruses, physically abusing hardware, altering source codes or software settings, etc.).

- Intentionally wasting resources.
- Sending or displaying offensive or inappropriate messages or pictures; using obscene language; harassing, insulting or attacking others.
- Violating copyright laws. The legal rights of software producers and network providers and copyright and license agreements must be honoured.
- Employing the network for commercial purposes or activities for institutions or organisations, product advertisement or political lobbying is prohibited.
- Using the network to disrupt its use by other individuals or by connecting networks.
- Disrespect of others' privacy and intellectual property.

Note:

1. The college network has audit trails. This means that student files and network activity are monitored regularly for any breach of this policy. Such breaches are reported to the Learning Technology Co-ordinator for appropriate action.
2. System Administrators must be notified of security problems which must not be demonstrated to other users.

Sanctions may include one or more of the following:

- Withdrawal of access privileges to the college network. (Note: there will be no exceptions for VCE students).
- Detention - community work for the college outside school hours. (e.g. cleaning computer rooms)
- Revocation of online access for breaches of online rules.
- Withdrawal from class; suspension; expulsion
- Law enforcement agencies may be involved.

SECTION B

BYOD POLICY

Sunbury College aims to provide students with the opportunity for more personalised learning by having access to digital technology at school. With the privilege of using their own device at the college, comes the responsibility to use the technology in a manner that is in keeping with our core values.

I understand that the following terms and conditions govern bringing my own device to the college:

1. Network and internet access

All content including but not limited to files, photos, videos and music must remain appropriate, as deemed by the college, at all times. The college retains the right to review the content of any device registered under this agreement. Content accessed through the internet will be subject to monitoring and filtering.

2. Power to recharge

Devices should arrive at the college fully charged as the college will not provide charging facilities. Chargers must not be brought to school. It is recommended that devices have a battery life of at least six hours.

3. Technical support

As the device is neither owned nor managed by the college, the college can only provide limited technical support.

4. Insurance and liability

It is strongly recommended that parents insure their child's device for loss or damage. The college accepts no responsibility for the loss or damage of the device. Devices must be stored securely and safely (in a

locker with a lock) when not in use. Personal devices are not covered by the college property insurance. They should not be left at school overnight.

5. Responsible use

The device must be used for educational purposes and in accordance with the acceptable use policy and other college rules. Any use of a device deemed inappropriate by the college may result in the withdrawal of BYOD privileges and other consequences as deemed appropriate by the college.

6. Hardware and Software requirements

The college prescribes minimum technical specifications for devices permitted under the BYOD policy. These requirements are subject to change from year to year. The minimum specifications for devices are outlined at the end of this agreement.

7. User Agreements

A wireless certificate will not be installed until the student has fully completed the required User Agreements attached to this document.

SECTION C

CYBERSAFETY, RESPONSIBLE ONLINE BEHAVIOUR AND ACCEPTABLE USE

Sunbury College believes the teaching of cybersafety and responsible online behaviour is essential in the lives of students and is best taught in partnership between home and school.

21st century students spend increasing amounts of time online, learning and collaborating. To be safe online and to gain the greatest benefit from the opportunities provided through an online environment, students need to do the right thing by themselves and others online and act respectfully, responsibly and appropriately, particularly when no one is watching.

Safe and responsible behaviour is explicitly taught at our school and parents/carers are requested to reinforce this behaviour at home. Some online activities are illegal and as such will be reported to police.

School Support for the Safe and Responsible Use of Digital Technologies

Sunbury College uses the college intranet, internet, and digital technologies as teaching and learning tools. We see the internet and digital technologies as valuable resources, but acknowledge they must be used responsibly. Parents/carers should be aware that the nature of the internet is such that full protection from inappropriate content can never be guaranteed.

At Sunbury College we:

- have policies in place that outline the values of the school and expected behaviours when students use digital technology and the internet
- provide a filtered internet service
- provide access to the Department of Education and Early Childhood Development's search engine Connect www.education.vic.gov.au/secondary which can be used to direct students to websites that have been teacher recommended and reviewed
- provide supervision and direction in online activities and when using digital technologies for learning
- support students in developing digital literacy skills
- are an E Smart school that looks at cybersafety in the curriculum and are continually developing our program
- use mobile technologies for educational purposes (e.g. podcasts or photos from excursions)
- provide support to parents/carers to understand this agreement (e.g. language support)
- provide support to parents/carers through information evenings and through the information in this booklet for parents to keep at home
- work with students to outline and reinforce the expected behaviours when working in a digital environment.
- do not disclose personal and sensitive information for non-school purposes or without parent consent.

Safe and Responsible Use of Digital Technologies

In signing the user agreement at the end of this booklet, your child will be agreeing to behave in a certain way online and to take appropriate action when and as required. Parents/carers will be countersigning the agreement. Elements of the agreement are explained below. Please contact the school to clarify or receive additional information.

At school the internet is mostly used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, but it is increasingly being used as a social space to meet and chat.

The term “space” is used here to describe a website that works like a community with live interaction and the capacity for your child to chat with others, personalise their space and share information. Each space has a purpose, audience and tool set including those around security and protection. The internet also provides access to websites with information, images and videos for students to view. Not all content is presented as a space.

Students should be safe, responsible and ethical users whenever and wherever they use digital technologies. The school’s Student Engagement/Wellbeing Policy, College Network Student Code of Conduct and Use of Mobile Phone / Camera Policy outline the values of the school and expected behaviours when students use digital technology. Key points include:

1. **Students should support others by being respectful in how they communicate with each other and never write or participate in online bullying (this includes forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviour).** Being online can make students feel that they are anonymous and sometimes students may say things online that they would never say to someone’s face. The web space or online chat environment that they use in leisure time might also have explicit language and they may feel they have to be part of it. Bullying online can take a number of forms from repeated messages to exclusion from social spaces. Students who forward on messages or participate in the exclusion may not see themselves as bullying. These actions also contribute to the hurt and distress of others and do constitute bullying.
2. **Students should talk to a teacher if they feel uncomfortable or unsafe online or see others participating in unsafe, inappropriate or hurtful online behaviour.** Incidents online often go unreported. Students have reported their reasons as embarrassment, a belief that online issues are theirs to solve as adults don’t understand, a feeling that reporting it will make it worse and the most common reason given is a fear that they will lose access to their technology.

   Students are advised to report an incident if:

   - they feel that the welfare of other students at the school is being threatened
   - they come across sites which are not suitable for their school
   - someone writes something they don’t like, or makes them and their friends feel uncomfortable or asks them to provide information that they know is private
   - they accidentally do something which is against the rules and responsibilities they have agreed to.
3. **Students should seek to understand the terms and conditions of websites and online communities and be aware that content they upload or post is their digital footprint.**

   Many websites/spaces have conditions of use, such as ownership of the content and the age of participants. For example: Children under 13 years of age are not permitted access to Facebook. When posting information online - A good rule is “Don’t post what you wouldn’t want your Grandparent, Principal, or future boss to read.”
4. **Students should protect their privacy rights and those of other students by not giving out personal details including full names, telephone numbers, addresses and images.**

   Students like to publish information about themselves and their friends in spaces like Twitter, Facebook and blogs. This can put them at risk of being approached, groomed or bullied online. To avoid this we recommend they:

   - don’t use their own name, but develop an online name and use avatars
   - don’t share personal details, including images of themselves or their friends online
   - password protect any spaces or accounts they have
   - don’t allow anyone they don’t know to join their chat or collaborative space
   - are reminded that any image or comment they put on the internet is now public (anyone can see, change or use it) so no full names should appear in reference to individuals in any image, movie or sound recording

- ALWAYS make the space private so that they can control who sees their space and can communicate with them
- understand the terms and conditions of any website or online community that they might join.
- teachers will outline expected processes with students in these spaces however, it is still important to think before you post to any online space.

5. **The internet at school should only be used for educational purposes and the equipment should be used properly.** It is important to realise that there is a time for fun and a time for work even on the internet. Students may often see the internet as 'free' however even just looking at a page on the internet incurs download traffic and consumes bandwidth. Accessing games on the internet is particularly heavy on internet traffic. By thinking carefully before downloading from the internet students can help the internet work more efficiently and save time, money and the environment. Staying on task will reduce the risk of inappropriate access and teach students strategies to use the internet or mobile technologies for their learning.
6. **Students should use social networking sites for educational purposes and only as directed by teachers.** Web 2.0 tools and social networking spaces allow students to be contributors to the web and to work collaboratively online with other students. Creating or contributing to blogs, wikis, digital stories and podcasts can all be legitimate educational activities which allow students to publish, share and inform others and be active contributors to the web. It is important for students to understand that working in a collaborative space as part of a learning task, has a very different purpose to using a social networking space to link up with friends in their own time. At a home with internet, students will be able to access their learning spaces. They will also have access to the rest of the internet. If your child is spending hours online 'doing their homework,' it may be that they are multitasking in many other applications, some of it study related and other interaction may be social.
7. **Students should abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary).** Music, information, images and games on the internet are owned by someone. The term copyright is a legal one and there are laws to enforce it. Not only is breaking copyright morally, ethically and legally wrong, it can introduce potential risks. By downloading a 'freebie' you can risk bringing a virus or spyware to the computer or system. These can destroy a computer system or provide hackers with details such as passwords and bank accounts. Peer to peer sharing of software like FrostWire and BitTorrent can sometimes share music and files illegally, and make computers vulnerable.
8. **Students should think critically about other users' intellectual property and how they use content posted on the internet, not simply copy and paste information from websites.** Not everything on the internet is true, accurate or unbiased. The school is working to teach digital literacy skills, which enable students to locate, evaluate, and use information effectively on the internet. It is important that your child respects the Intellectual Property of people who contribute resources online. Students should use their own thoughts and language to express what they have learnt, and avoid simply copying and pasting information from the internet.
9. **Students should follow accepted classroom protocols as outlined by their teacher when working in a 1:1 environment.** The college is developing protocols to be used across all classes. To ensure students understand the difference between an educational collaborative space and a community dedicated to socialising, teachers will clearly outline the educational purpose of the task and the roles and responsibilities of students. Protocols for what will be considered acceptable practice in the collaborative space and in the classroom will be established, especially when the work requires sharing of space.
10. **Students should not:**
    - Interfere with network security, the data of another user or attempt to log into the network or internet with a user name or password of another student.
    - Reveal their password or wireless certificate details to anyone.
    - Use another student's device or allow another student to use their device.

- Deliberately enter or remain in any site that has obscene language or offensive content (e.g. racist material or violent images).
- Use a device to capture photos or videos of other members of the college community without their consent

In school settings, internet service providers set up filters to block out a lot of inappropriate content, but these filters are not always foolproof. Students who deliberately seek out inappropriate content or use technologies which bypass filters, will have their internet access reviewed and their parent/carers will be informed where appropriate.

The recording of images and sounds can breach students' rights under the Privacy Act. Sometimes students are reluctant to tell their peers that they don't want their image or voice recorded. The Privacy Act says that the posting and sharing of private information online or in any other way requires consent.

When using digital devices students should:

- Follow the relevant policies including the mobile phone policy and subject specific policies when using college resources.
- Only take photos and record sound or video when it is part of a class or lesson and explicit teacher permission has been given.
- Seek permission from individuals involved before taking photos, recording sound or videoing them (including teachers).
- Seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space.
- Be respectful in the photos they take or videos they capture and never use these as a tool for harassment.

- If you have any concerns about this agreement contact the school.
- For further support with online issues students can call Kids Helpline on 1800 55 1800. Parents/carers call Parentline 132289 or visit http://www.cybersmart.gov.au/report.aspx

Appendix A: Minimum Specifications for BYOD Devices

Below is the list of minimum specifications (standards) that must be met for a device to be connected to the school network. If you are unsure about the specifications of your device, contact our IT department who may be able to help identify if your device is suitable.

Permitted Devices and Minimum Requirements

- Laptop functionality refers to a full size keyboard with the ability to run either OSX or Microsoft Windows
- Laptops Specifications (Windows based machines are strongly recommended)
  - 4GB of RAM
  - 128 GB of Storage
  - i3 Processor or greater (or equivalent)
  - Screen of at least 12” or more
  - Touch screen with a stylus (Optional but highly recommended)
- The battery life of devices must be 4 hours or more (students are not permitted to charge their device in class due to OH&S requirements)

Approved Operating Systems compatible with the College network

- Windows 10* (recommended), OSX 10.13/High Sierra and up (Apple)

*Windows 10 S (basic version) is not supported. Please upgrade to the Full version of Windows 10

The Sunbury College Network Student code of conduct and BYOD User Agreement applies during school, school excursions, camps and extra-curricular activities. The User Agreement must be signed and provided to the school along with initial enrolment forms.

About this User Agreement

This document has been developed to assist the school community in understanding the college policy regarding the Network Student Code of Conduct, BYOD and other digital technologies.

Parents/carers and students should carefully read through this booklet before signing the User Agreement and Permission forms.

USER AGREEMENT AND PERMISSION FORM

As a user of the Sunbury College computer network, I hereby agree to comply with the College Network Student Code of Conduct and BYOD policy. I will use the network and equipment responsibly, employing good user practices and ethics and honouring all relevant laws and restrictions. I understand that any breach of these conditions will result in Network Access and BYOD privileges being suspended or revoked and other possible consequences as deemed appropriate by the college.

Student name: _____ Year Level:_____

Signature: _____ Date: _____

As the parent or legal guardian of the user signing above, I grant permission for my child to access the college network and to use the services it provides including electronic mail, the internet and intranet. I have read the Sunbury College Network Student Code of Conduct and BYOD Policy carefully and I understand that users may be held liable for violations of these policies. I understand that some materials on the internet may be objectionable and accept responsibility for guidance of internet use for my child when selecting, sharing or exploring information. I understand that any breach of these conditions will result in Network Access and BYOD privileges being suspended or revoked and other possible consequences as deemed appropriate by the college.

Parent Signature:_____ Date: _____

PLEASE RETURN THIS PAGE TO THE COLLEGE WITH YOUR ENROLMENT FORMS AFTER YOU HAVE TAKEN A PHOTOCOPY FOR YOUR RECORDS.